INTEROPERABLE SIMULATION FOR PROTECTING PORT AS CRITICAL INFRASTRUCTURES

Agostino Bruzzone[(a)], Alberto Tremori[(a)], Francesco Longo[(b)]

[(a)] DIME, University of Genoa, Italy - www.itim.unige.it
[(b)] MSC-LES, Mechanical Dept, University of Calabria, Italy – www.msc-les.org

[(a)]agostino@itim.unige.it, alberto.tremori@simulationteam.com, [(b)]f.longo@unical.it

ABSTRACT

The research proposes an interoperable simulation framework to analyze and investigate security issues in complex maritime scenarios affected by asymmetric threats (i.e. terrorist attacks) with particular attention to people and goods flows in Ports. The main aim is to support both decision makers and trainers in applying operational and organizational security policies and procedures and to assess the impact of these policies on security efficiency in global flows of goods & people. Therefore the proposed framework is useful for the review, testing and certification of Ports Security Plans, Risk Assessments and Gaps Identification as well as for operators training.
Due to the complexity of the Port system including several actors and infrastructures, the operations coordination is critical in order to face new asymmetric threats; so interoperable simulation combined with Intelligent Agents and Data Fusion techniques is an important approach in order to provide a set of simulation models cooperating in the same scenario and to simulate security procedures and policies.
The authors provide a simulation federation to analyze and test security procedures and regulations by proposing a case study based on the collision of two hijacked ships within the port.

Keywords: Port Security, Interoperable Simulation, Intelligent Agents, Computer Generated Forces, Data Fusion.

INTRODUCTION

Considering new asymmetric threats such as terroristic and cyber attacks, fire explosions on board, shore fires, on-water spillage and environmental incidents within the port, Port Protection and Security are becoming very critical issues for the global maritime context (Alberts et al. 2000). In particular after the 9/11 terrorist attack, the security became suddenly the main problem for people and for the supply chain management, instead of the speed and efficiency of international trade and travel (Bruzzone 2010).
In effects international regulations and procedures are provided, such as:

- January 2002 Container Security Initiative (CSI)
- November 2002 Maritime Transportation Security Act of 2002 (MTSA)
- December 2002 International Convention for the Safety of Life at Sea (ISPS)
- July 2004 International Convention for the Safety of Life at Sea (SOLAS).

Therefore it is fundamental to assess critical situations and threats and to test different procedures and solutions (Bruzzone et al. 1997, Bruzzone et al 2010). Modeling and Simulation allows to reproduce different maritime scenarios involving several entities and actors (Merkuryev et al. 1998). In effect a Port is a complex system involving a large number of entities dynamically interacting in an open environment 24 hours/day 365 days/year (i.e. Coast Guard or Navy, Port Authority, Terminal Operators, Shipping Companies, Custom and Border Protection Agencies and other institutions).
Obviously, it is fundamental a good interaction and coordination among all the involved actors and facilities to successfully identify and respond to the threat; for this reason, new technologies and solutions are necessary to train operators and to test different security procedures and regulations without the block of port activities.
In addition a terrorist attack or and incident within the port could affect these actors and the whole logistic network which the port belongs, having a strong impact on global shipping and international trade as well as on port military strategies and local logistics and transportation system (Bruzzone et al. 1996). So, Security policies and procedures have a big impact on the transportation system. It is evident that if physical inspections (i.e. container scanning, gate controls, custom checks, etc.) are increased, it is possible to bring international trade to a halt or loose

competitiveness versus other countries. In this context, research should provide innovative solutions and technology to be applied to security procedures and operations (Bruzzone, Page & Uhrmacher 1999).
The authors propose a synthetic environment based on interoperable simulation models, combined with Intelligent Agents for Computer Generated Forces, in order to support Port authorities, Port safety officers, Vessel commanders, shipping companies and other departments (dealing with port issues) in analyzing and testing security plan and procedures and even in designing new ones (Bruzzone et al. 2005). In addition, this simulation should aid decision makers to quantify the trade-off between achieving security goals and their costs, as well as discovering improved procedures in order to optimize the performance of security systems, including all port activities and processes (i.e. material handling, data communication, human procedures, business processes, etc) (Curcio & Longo 2009).

1. THE SCENARIO

Port Protection is very difficult due to different factors:
- Its extension and size
- The excessive access ways, often not adequately monitored
- Lack of coordination and communication among different terminal operators that are assigned to protect different areas and docks
- Ferry and cruise terminals are open to the public
- Baggage are not always inspected on ferries
- Entrance is permitted also to un-authorized persons (passengers, suppliers, crews)
- Boats and tourism facilities are in close contact with operative areas
- Cargo handling involves check procedures and documentations that slow down operations

In the last years different threats and incidents are spreading including:
- Thefts
- Smuggling
- Narcotics
- Terrorism
- Fraud
- Clandestine individuals
- Vandalism
- Organized crime
- Environmental crime

To prevent and detect these threats it is necessary to focus on regulations and standards, organization and procedures and personnel training in order to proper react by taking into account (Fischer & Green 2003; Liddy 2005)
- Threat Intensity
- Alert Levels
- Inspections
- Planning
- Operative Support control

These standards introduce actions and preventions to be carried out in order to improve port security:
- inspections to protect global trade system
- intelligence use and automated advance targeting information to identify and target containers that pose a risk for terrorism
- Prescreening those containers that pose a risk at the port of departure
- Improve communication among law enforcement officials responsible for port security
- to invest in long-term technology
- to increase intelligence collection on cargo and intermodal movements
- to conduct vulnerability assessments and develop security plans that may include passenger, vehicle and baggage screening procedures; security patrols; establishing restricted areas; personnel identification procedures; access control measures; and/or installation of surveillance equipment.

2. M&S FOR SECURITY IN MARITIME CONTEXT

Modeling & Simulation provides a very fundamental support to Port Security in different application areas:
- Architecture/Infrastructure/Procedure Design
- Training
- Testing New Solutions
- Standing Operation Planning
- Operative Support & Emergency Management

In addition M&S supports port authorities to improve infrastructure design, control system architecture and operation management by considering security requirements and regulations and to reduce the impact of new threats within reasonable cost and without losing operative efficiency (Sennewald 2003; Longo et al. 2012).
The use of M&S to analyze and improve security within a port is more than justified by the need to analyze complex interactions among numerous factors. The simulation techniques are actually employed to evaluate impacts of the security requirements for people flow (e.g. passenger and baggage screening on port operations performance) and cargo flow. In particular Security equipment and procedures related to logistics facilities are usually grouped into:
- Internal: Security control of logistics flow to ensure that goods are not dangerous (i.e. container scanning, gate controls, custom checks, etc.)
- External: Security control of external component (i.e. terrorists)

In addition it is necessary to consider that the intensive flows of entities (i.e. people, materials, etc.) in logistics facilities have a mutual influence and can be a potential

threat to other entity flows. For instance in port logistics there are several entities, that are potential threat; in this domain, intrusion models could be used to control potential interference between Cargo and people entities in various areas of ports and M&S is often used to study processes, performance levels and costs with regard to regular operating conditions and to support assessments of the impact of safety and security procedures on logistics results (Bruzzone & Giribone 1998). These simulators are also used to test different organizational models within critical structures (Bruzzone 2004).

Several tools are available in the commerce for port infrastructures and logistics simulation (i.e. RescueSim and PortSim); anyway as far as we know, no one of them allows an integrated approach to quantify the economical impact of the different security policies, and to offer a decision support tool to improve security procedures while minimising a cost increment to the production industry.

New enabling technologies have a great potential in the maritime context (Ladner & Petry 2005); for instance communication infrastructures and mobile solutions allows today to distribute information as well as data collection, data processing and decision making over a large complex network and even great benefits are provided by innovative soft computing techniques and methodologies (Anderson, 2006; Bruzzone et al., 2011b,; Bruzzone, Page and Uhrmacher, 1999; Ladner et al., 2009).

In the recent years the authors are studying new models and solutions based on a multi dimension and multi layer resolution by taking into account the Real World 5 Dimensions (Surface, Underwater, Air, Space, Cyber) and different layers & Resolutions Frame such as Fleets and Parties, Ships and Commercial Traffic, Crew & People Acceding Ports/Vessels, Services & Infrastructures. In addition it is necessary to consider critical issues such as (Bruzzone 2010):

- Non Conventional Operations
- Human Behaviors on (i.e. Crew, Stakeholders, Domestic Opinion)
- Services & Infrastructures
- Commercial Traffic & Yachting
- Port Infrastructures and Resources
- Joint Operations (i.e. Ship Inspections, Littoral Control, C5I2)

The authors have great experience in the use of Modeling and Simulation to reproduce complex maritime scenarios affected by asymmetric threats such as Piracy, Conventional Terrorism, CBRN (Chemical, Biological, Radiological and Nuclear) (Bruzzone et al. 2011, Bruzzone 2010). Threats and in the development of simulation models integrated by using HLA Standards (High Level Architecture), by taking into account all the previous mentioned aspects.

In particular this paper is focused on a solution including:

- **Cognitive Technologies** (i.e. Data Fusion, Human Behaviour Modelling, Intelligent Agents & CGF)
- **Modelling & Simulation** (i.e. interoperable Simulation, virtual environment, etc.)
- **Equipment & Devices** (i.e. Integrated Solutions)

The authors propose a federation of simulation models devoted to test and evaluate security procedures and to demonstrate M&S potential within marine asymmetric scenarios. In particular the research is inspired to a previous European R&D Project "GLOWS" where the authors were involved (Bruzzone 2005). GLOWS was devoted to identify needs and gaps in the following areas (Bruzzone et al. 2009):

- Biometrics Research: computational biomedicine, computer vision, computer graphics and deformable algorithm.
- Cyber Attacks of Transportation
- Wireless non human entities are being placed as elements of cyber space.

In similar way, GLOWS faces important points in freight handling, with special attention to Passenger and Container inspection procedures, currently requiring to be improved by introducing innovative technologies and new processes paying in attention security:

- Queuing models and inventory control analytical and simulation methodologies;
- Risk Factors for containerised cargo;
- Data mining and analysis on People and Material Flows. Bayesian methods;
- Standardised data submission;

In this research the authors propose a simulation framework based on the following previous experiences such as (Bocca et al. 2007; Bruzzone et al. 2004; Bruzzone 2007; Bruzzone et al. 2011):

- **IA-CGF & Human factors** for maritime security: models reproducing human factors and representing intelligent agents able to direct objects within interoperable simulators; these new *IA-CGF* (Intelligent Agents for Computer Generated Forces) modules are interoperable in HLA Federation (High Level architecture) and they include: IA-CGF Units (i.e. commercial ships, contractors on the ship, special teams, fisherman boats, coast guard units); IA-CGF HBL Human Behavior Libraries (i.e. fatigue, stress, aggressiveness, trustiness); IA-CGF NCF Non-Conventional Frameworks devoted to reproduce specific scenarios (i.e. piracy).
- ***PANOPEA:*** a simulation model based on intelligent Agents (IA) able to reproduce a complex framework related to piracy involving several thousands of vessels, plus all related activities (i.e. intelligence, ports, special forces, contractors, helicopters, UAV, etc.) (Bruzzone et al. 2011).

Figure 1. IA-CGF NCF and PANOPEA simulators

- ***PLACRA:*** simulator devoted to reproduce the crew activities and behavior on Oil Platforms as well as on vessels
- ***MESA:*** an integrated environment devoted to perform simulation and risk analysis in ports and maritime sector considering the evolution of emergencies (Bruzzone et al. 1999)
- ***FLODAF:*** tool devoted to support engineering and performance estimation of Data Fusion architectures and algorithms for analyzing the Data Fusion performances over complex Air-Naval scenarios including surface and underwater vessels, aircrafts.
- ***ST-VP:*** developed as a framework to support Training in marine environments; ST-VP includes all the different port equipment and even other marine devices and platforms

Figure 2. PLACRA, MESA, FLODAF and ST-VP Simulators

In the paper the authors propose a federation based on a synthetic environment and focusing on Safety and Security Training, Procedure Definition, Equipment Design and Virtual Prototyping.

3. SIMULATION MODEL AND POTENTIAL BENEFITS FOR PORT SECURITY

The authors propose a simulation framework to support the analysis and assessment of security procedures and plans within a port.
The framework includes:

- a synthetic environment reproducing the port facilities and components
- IA-CGF HBM to simulate the human factors affecting the activities of the vessels, boats, airplanes, coast infrastructures (i.e. crew behavior)
- IA driving the general traffic and critical entities (i.e. airplanes, yachts, ships, ground entities reacting dynamically to the Simulation Evolution)
- IA directing actions for the Port and Coast Protection
- IA directed Models reproducing Naval Resources, including platforms, weapons, individual sensors, ground infrastructures, C2 (Command and Control) and different information

The purpose is to develop innovative solutions, for port security improvement, able to:
- identify, analyze and reproduce "Intelligent Behaviors" by conservative and smart use of sensors, adopting behavior of general traffic, compromising info source, grouping and desegregating on the coast
- have Capabilities in Scenario Awareness
- have Capabilities in term of Autonomy
- have Capabilities in Coordinating different Agents

Considering, as example, the collision of two hijacked ships in a port, this scenario should include the following entities:

- The two ships (i.e. two cargo ships)
- Crew and Human Factors
- Other cargo ships, fishing ships and vessels driven by intelligent agents
- Coast Guard
- Port Authority
- Ambulance
- Local Police and government agencies
- Intelligence Agencies
- Sensors for threats detection
- Weapon Systems
- Threats
- External Traffic
- Logistics Infrastructures
- Litoral Resources

The federation architecture is proposed below:

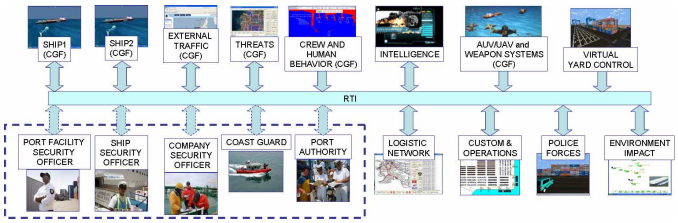

Figure 3. Federation Architecture

Particular attention is focused on the security responsible; these roles (mentioned in ISPS code) could be played by humans in order to define security plan and to act based on scenario evolution.
The proposed model is able to support both decision making and training. Due to interoperability features, this framework provides several benefits such as:

- Make more effective security procedures and plan
- Capability to discover or develop new security procedures
- Capability to quantify security procedures effectiveness in term of costs, time of threat detection, time of threat reduction or elimination
- Improve personnel coordination and communication
- Improve Personnel awareness and knowledge about security procedures

4. CONCLUSIONS

Harbour and Maritime Security is part of a wide Scenario and need to be addressed by an integrated approach. Marine Asymmetric Warfare is fast evolving introducing new issues and new threats affecting more and more subjects. Standards and Regulations exist but emerging technologies are key issues for investigating this domain respect new threats and supporting development of New Systems, Devices and Equipment but in particular personnel education. The research addresses the aspects mentioned above and proposes a simulation framework based on integrated approach and interoperability standards to support decision makers and trainees in applying security standards and procedures taking into account costs and security effectiveness. Existing solutions developed by authors could (coming also from industrial experiences (Bruzzone et al. 2011)be combined and integrated in order to create this simulation framework, allowing personnel training and port efficiency analysis.
It is evident that today simulation makes security issues opportunities to redesign logistics operations and infrastructures and facilities by testing new solutions and enabling technologies that are able to support this process.
In this context M&S provides quantitative support to decision makers for identifying solutions able to reduce the impact of the new threats with reasonable costs and without loosing operative efficiency.

REFERENCES

Alberts David S., Gartska J.J., Stein F.P. (2000) "Net Centric Warfare", CCRP, Washington

Bocca E., Pierfederici, B.E. (2007) “Intelligent agents for moving and operating Computer Generated Forces” Proceedings of SCSC, San Diego July

Bruzzone A.G., Massei M. Tremori A., Longo F., Madeo F., Tarone F, (2011) “Maritime Security: Emerging Technologies for Asymmetric Threats”, Proceedings of EMSS2011, Rome, Italy, September 12 -14

Bruzzone A.G., Massei M., Madeo F., Tarone F. (2011) "Simulating Marine Asymmetric Scenarios for testing different C2 Maturity Levels", Proceedings of ICCRTS, Quebec, Canada, June

Bruzzone A.G. Tremori A., Massei M. (2011) "Adding Smart to the Mix", Modeling Simulation & Training: The International Defense Training Journal, 3, 25-27, 2011

Bruzzone A.G., Massei M. Tremori A., Madeo F., Tarone F, Gazzale G. (2011) “Modeling and Simulation as Support for Decisions Making in Petrochemical Marine Logistics”, Proceedings of HMS2011, Rome, Italy, September 12 -14

Bruzzone A.G., Tremori A., Merkuryev Y. (2011) “Asymmetric marine warfare: PANOPEA a piracy simulator for investigating new C2 solutions” Proceedings SCM MEMTS 2011, St.Petersburg June 29-30

Bruzzone A.G. (2010) "CGF & Data Fusion for Simulating Harbor Protection & Asymmetric Marine Scenarios", Proceedings of SIM&SEA2010, La Spezia, June 8

Bruzzone A.G., Tremori A., Bocca E., (2010) "Security & Safety Training and Assessment in Ports based on Interoperable Simulation", Proceedings of HMS2010, Fes, Morocco, October 13-15

Bruzzone A.G. (2005) "GLOWS", DIPTEM Press Genoa, Italy

Bruzzone A.G., Viazzo S., Massei M., (2004) "Modelling Human Behaviour in Industrial Facilities & Business Processes", Proc. of ASTC, Arlington, VA, April

Bruzzone (2004). Preface to modeling and simulation methodologies for logistics and manufacturing optimization . SIMULATION, vol. 80 , p. 119-120 , ISSN: 0037-5497, doi: 10.1177/0037549704045812

Bruzzone A.G., Page E., Uhrmacher A. (1999) "Web-based Modelling & Simulation", SCS International, San Francisco, ISBN 1-56555-156-7

Bruzzone A.G., Rapallo S., Vio F., (1999) "MESA: Maritime Environment for Simulation Analysis", Tech.Report of ICAMES, ENSO, Bogazici University, Istanbul, May 15-21

Bruzzone A.G., Giribone P. (1998) "Decision-Support Systems and Simulation for Logistics: Moving Forward for a Distributed, Real-Time, Interactive Simulation Environment", Proc. of the Annual Simulation Symposium IEEE, Boston

Bruzzone A.G., Cotta G., Cerruto M. (1997) " Simulation & Virtual Reality To Support The Design Of Safety Procedures In Harbour Environments ", Proceedings of ITEC97, Lausanne (CH), April 22-25

Bruzzone A.G., Giribone P., Mosca R. (1996). Simulation of Hazardous Material Fallout for Emergency Management During Accidents. SIMULATION, vol. 66 (.6), p. 343-355, ISSN: 0037-5497CTA (2002) "Agents for Net-Centric Warfare and Time Critical Targets", CTA Technical Report

Curcio D, Longo F (2009). Inventory and Internal Logistics Management as Critical Factors Affecting the Supply Chain Performances. International Journal of Simulation & Process Modelling, vol. 5(4), p. 278-288, ISSN: 1740-2123

Fischer R., Green G. (2003) “Introduction to Security”, Butterworth-Heinemann

Ladner R., Petry F. (2005) "Net-Centric Web Approaches to Intelligence and National Security", Springer, NYC

Liddy L. (2005) "The Strategic Corporal: Some Requirements in Training and Education", Australian Army Journal, Volume II, Number 2, 139-148

Longo F, Massei M, Nicoletti L (2012). An application of modeling and simulation to support industrial plants design. International Journal of Modeling, Simulation, and Scientific Computing, vol. 3, p. 1240001-1-1240001-26, ISSN: 1793-9623, doi: 10.1142/S1793962312400016

Merkuriev Y., Bruzzone A.G., Novitsky L (1998) "Modelling and Simulation within a Maritime Environment", SCS Europe, Ghent, Belgium, ISBN 1-56555-132-X

Merkuryev Y., Bruzzone A.G., Merkuryeva G., Novitsky L., Williams E. (2003) "Harbour Maritime and Multimodal Logistics Modelling & Simulation 2003", DIP Press, Riga, ISBN 9984-32-547-4 (400pp)

Marine Log (2004) "Jitters as ISPS/MTSA deadline nears", Simmons-Boardman Publishing Corporation, Omaha

Marine Log (2004) " MTSA and ISPS: final rules issued", Simmons-Boardman Publishing Corporation, Omaha

Marine Log (2003) "IMO wants early ISPS implementation", Simmons-Boardman Publishing Corporation, Omaha

Ray D.P. (2005) "Every Soldier Is a Sensor (ES2) Simulation: Virtual Simulation Using Game Technology", Military Intelligence Professional Bulletin

Shahbazian E., Rogova G., Weert M.J. (2009) "Harbour Protection Through Data Fusion Technologies", Series: NATO Science for Peace and Security Series C: Environmental Security, Springer

Safety at Sea International (2003) "What will be the cost of ISPS? As ports and shipping companies race to comply with an extremely tight deadline to meet the IMO security requirements", DMG World Media, London

Security Management (2003) "IMO sets course for port security", American Society for Industrial Security, Alexandria

Sennewald C. (2003) “Effective Security Management”, Butterworth-Heinemann

Tyska L., Fennelly L. (2001) “Cargo Theft Prevention: A Handbook for Logistics Security”, American Society for Industrial Security